

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel E. Zaehring, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since 2010, and am currently assigned to the HSI Bangor, Maine office. Since 2015, I have investigated crimes involving the use of computers and the Internet and have investigated crimes involving the sexual exploitation of children. I have participated in the execution of numerous search warrants, both residential and online accounts, and the seizure of computers, cell phones, electronic media, and other items evidencing violations of federal laws pertaining to the sexual exploitation of children. I have also participated in numerous arrests and interviews of subjects involved with child exploitation and/or child pornography and have review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As an HSI agent, I am authorized to conduct these investigations and to request and execute search warrants for evidence of violations of Title 18 of the United States Code.

2. This affidavit is submitted in support of an application for a search warrant for the locations specifically described in Attachment A of this Affidavit and any devices seized, including the entire property located at 364 North Street, Calais, Maine 04619

(the “SUBJECT PREMISES”), described vehicle, and the person of Eric Muise for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A, which is more specifically described in Attachment B of this Affidavit.

3. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience. Based on this training and experience, there is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography); §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); and 18 U.S.C. § 2251 (production of child pornography), are presently located at the locations described in Attachment A.

#### **STATUTORY AUTHORITY**

4. As noted above, this investigation concerns alleged violations of the following:

- a. Title 18, United States Code, Sections 2252A(a)(5)(B) prohibits a person from possessing child pornography that has been transported in interstate commerce or

produced using materials that have been mailed, shipped or transported in interstate commerce;

b. Title 18, United States Code, Sections 2252A(a)(1) and (b)(1) prohibit a person from knowingly transporting in interstate commerce child pornography, as defined in 18 U.S.C. § 2256(8), including by computer.

c. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Section 2251 prohibits a person from employing, using , persuading, inducing, enticing, or coercing any minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, if that visual depiction was transported in interstate commerce or produced using materials that have been mailed, shipped or transported in interstate commerce.

#### **BACKGROUND ON KIK**

5. Kik Messenger (hereinafter “Kik”) is a free, instant messaging application which allows users to text, chat and share photographs, videos, and other information with other Kik users. When creating a Kik account, users are required to provide basic contact and personal identifying information. The information may include the user’s full name, birth date, contact email address, Kik password, screen names, and other personal identifiers. Email addresses can be “confirmed”, which means the user verified that the email address is valid by clicking a link sent from Kik to the provided email address, or “unconfirmed”, which means the email address is invalid, or the user did not verify the email address by clicking on the link from Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process. During this process, the user selects/creates a Kik username which is a unique identifier which can never be replicated. Kik also retains IP logs for each user which include the IP address, date and time of the user’s Kik account access.

6. Kik provides a platform for finding people who are available to chat and have similar interests. Users can send out an open invitation, search for specific users, or seek out new friends based on their profile details. Kik users may also join one or more groups or chatrooms to connect and interact with other users who are members of the same group.

7. Information stored in connection with a Kik account may provide evidence of the “who, what, why, when, where, and how” of the criminal conduct under

investigation, thus enabling law enforcement to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Based on my training and experience, I know that a Kik user's IP log, stored electronic communications, and other data retained by Kik can indicate who has accessed or controlled the Kik account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Thus, any device used to access Kik is likely to contain the information described above, including any stored electronic communications.

#### **PROBABLE CAUSE**

8. On September 22, 2021, the Homeland Security Investigations, Cyber Crimes Center (hereinafter "HSI C3") referred an investigative lead to me regarding a Kik user who had chatted about the sexual abuse of children, specifically their two-year-old daughter, and to taking photos of her genitals. This chat occurred between September 10, 2021, and September 13, 2021. As part of the chat, the user posted a facial photo of a child they claimed to be their daughter as well as a picture of children's underwear, pictures of what they claimed to be their child's bedroom and playroom, and a picture of the child's vulva. HSI C3 identified the Kik account as "Screenname 1"<sup>1</sup> and obtained subscriber information and IP login history for this account from Kik. HSI C3

---

<sup>1</sup> The actual screennames have been substituted with "Screenname" and a number ("1", "2" etc.) to preserve the integrity of ongoing investigations. This naming convention will continue for subsequently referenced screennames.

determined that the user of the account likely lived in Calais, Maine based on the IP address used to access the account. HSI C3 forwarded the lead information to me for further investigation.

9. On September 23, 2021, I reviewed the lead information which contained Kik subscriber data and IP login history for the “Screenname 1” account, a Kik message thread, and Charter Communications IP address subscriber information. I began my investigation by reviewing the Kik message thread and noted that “Screenname 1” corresponded with the administrator of a parent’s group in order to gain access to the group.

10. On September 10, 2021, “Screenname 2” direct messaged “Screenname 1” regarding “Screenname 1” accessing the group. The relevant messages are as follows:

Screenname 2: I admin a small all verified parent group. To share lives and candid of our children. Pm if interested and can verify to be added xx.

Screenname 2: So did you want to verify?

Screenname 1: What do you need again

Screenname 2: [Entry Requirements redacted<sup>2</sup>]

---

<sup>2</sup> The group entry requirements are redacted to preserve the ongoing investigation

Screenname 1: [Picture posted which depicts an approximately 3-year-old girl standing at a table. The face of the child is clearly visible and the child is wearing pink clothing with white hearts on it]


Screenname 1: [Picture posted of someone's hand holding a pair of children's underwear]

Screenname 1: Won't be able to do her room until her mom leaves

Screenname 2: Ok. No rush. I can ask the other bits. How old? Daught and do you play with her or just panties? Mine are 6 and 9, girls.

Screenname 1: She's 3 in three weeks is that to young

Screenname 1: And I touch her when I'm alone and can

Screenname 2: That is perfect age. You touching the cunny or ass or both  
.

Screenname 1: Bath

Screenname 2: Do you take pics of her like cs stuff or you only do the playing? She not be youngest in the group

Screenname 1: Only playing. I try and get creep shots for groups of her butt and cunny

Screenname 2: We don't ask anyone to do anything they aren't already doing for the group. But others peeps do that too. What kind of stuff you share in other groups just her butt and cunny?

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel E. Zaehring, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since 2010, and am currently assigned to the HSI Bangor, Maine office. Since 2015, I have investigated crimes involving the use of computers and the Internet and have investigated crimes involving the sexual exploitation of children. I have participated in the execution of numerous search warrants, both residential and online accounts, and the seizure of computers, cell phones, electronic media, and other items evidencing violations of federal laws pertaining to the sexual exploitation of children. I have also participated in numerous arrests and interviews of subjects involved with child exploitation and/or child pornography and have review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As an HSI agent, I am authorized to conduct these investigations and to request and execute search warrants for evidence of violations of Title 18 of the United States Code.

2. This affidavit is submitted in support of an application for a search warrant for the locations specifically described in Attachment A of this Affidavit and any devices seized, including the entire property located at 364 North Street, Calais, Maine 04619



(the “SUBJECT PREMISES”), described vehicle, and the person of Eric Muise for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A, which is more specifically described in Attachment B of this Affidavit.

3. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience. Based on this training and experience, there is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography); §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); and 18 U.S.C. § 2251 (production of child pornography), are presently located at the locations described in Attachment A.

#### **STATUTORY AUTHORITY**

4. As noted above, this investigation concerns alleged violations of the following:

- a. Title 18, United States Code, Sections 2252A(a)(5)(B) prohibits a person from possessing child pornography that has been transported in interstate commerce or

produced using materials that have been mailed, shipped or transported in interstate commerce;

b. Title 18, United States Code, Sections 2252A(a)(1) and (b)(1) prohibit a person from knowingly transporting in interstate commerce child pornography, as defined in 18 U.S.C. § 2256(8), including by computer.

c. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Section 2251 prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, if that visual depiction was transported in interstate commerce or produced using materials that have been mailed, shipped or transported in interstate commerce.

#### **BACKGROUND ON KIK**

5. Kik Messenger (hereinafter “Kik”) is a free, instant messaging application which allows users to text, chat and share photographs, videos, and other information with other Kik users. When creating a Kik account, users are required to provide basic contact and personal identifying information. The information may include the user’s full name, birth date, contact email address, Kik password, screen names, and other personal identifiers. Email addresses can be “confirmed”, which means the user verified that the email address is valid by clicking a link sent from Kik to the provided email address, or “unconfirmed”, which means the email address is invalid, or the user did not verify the email address by clicking on the link from Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process. During this process, the user selects/creates a Kik username which is a unique identifier which can never be replicated. Kik also retains IP logs for each user which include the IP address, date and time of the user’s Kik account access.

6. Kik provides a platform for finding people who are available to chat and have similar interests. Users can send out an open invitation, search for specific users, or seek out new friends based on their profile details. Kik users may also join one or more groups or chatrooms to connect and interact with other users who are members of the same group.

7. Information stored in connection with a Kik account may provide evidence of the “who, what, why, when, where, and how” of the criminal conduct under

investigation, thus enabling law enforcement to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Based on my training and experience, I know that a Kik user's IP log, stored electronic communications, and other data retained by Kik can indicate who has accessed or controlled the Kik account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Thus, any device used to access Kik is likely to contain the information described above, including any stored electronic communications.

#### **PROBABLE CAUSE**

8. On September 22, 2021, the Homeland Security Investigations, Cyber Crimes Center (hereinafter "HSI C3") referred an investigative lead to me regarding a Kik user who had chatted about the sexual abuse of children, specifically their two-year-old daughter, and to taking photos of her genitals. This chat occurred between September 10, 2021, and September 13, 2021. As part of the chat, the user posted a facial photo of a child they claimed to be their daughter as well as a picture of children's underwear, pictures of what they claimed to be their child's bedroom and playroom, and a picture of the child's vulva. HSI C3 identified the Kik account as "Screenname 1"<sup>1</sup> and obtained subscriber information and IP login history for this account from Kik. HSI C3

---

<sup>1</sup> The actual screennames have been substituted with "Screenname" and a number ("1", "2" etc.) to preserve the integrity of ongoing investigations. This naming convention will continue for subsequently referenced screennames.

determined that the user of the account likely lived in Calais, Maine based on the IP address used to access the account. HSI C3 forwarded the lead information to me for further investigation.

9. On September 23, 2021, I reviewed the lead information which contained Kik subscriber data and IP login history for the “Screenname 1” account, a Kik message thread, and Charter Communications IP address subscriber information. I began my investigation by reviewing the Kik message thread and noted that “Screenname 1” corresponded with the administrator of a parent’s group in order to gain access to the group.

10. On September 10, 2021, “Screenname 2” direct messaged “Screenname 1” regarding “Screenname 1” accessing the group. The relevant messages are as follows:

Screenname 2: I admin a small all verified parent group. To share lives and candid of our children. Pm if interested and can verify to be added xx.

Screenname 2: So did you want to verify?

Screenname 1: What do you need again

Screenname 2: [Entry Requirements redacted<sup>2</sup>]

---

<sup>2</sup> The group entry requirements are redacted to preserve the ongoing investigation

Screenname 1: [Picture posted which depicts an approximately 3-year-old girl standing at a table. The face of the child is clearly visible and the child is wearing pink clothing with white hearts on it]

Screenname 1: [Picture posted of someone's hand holding a pair of children's underwear]

Screenname 1: Won't be able to do her room until her mom leaves

Screenname 2: Ok. No rush. I can ask the other bits. How old? Daught and do you play with her or just panties? Mine are 6 and 9, girls.

Screenname 1: She's 3 in three weeks is that to young

Screenname 1: And I touch her when I'm alone and can

Screenname 2: That is perfect age. You touching the cunny or ass or both



Screenname 1: Bath

Screenname 2: Do you take pics of her like cs stuff or you only do the playing? She not be youngest in the group

Screenname 1: Only playing. I try and get creep shots for groups of her butt and cunny

Screenname 2: We don't ask anyone to do anything they aren't already doing for the group. But others peeps do that too. What kind of stuff you share in other groups just her butt and cunny?

Screenname 2: Sounds like you will enjoy our group 😊

Screenname 1: Yeah basically. Just a live shot then delete cuz my wife would murder me.

Screenname 1: Whats the youngest this group has and oldest

Screenname 2: I bet so would mine. I love the idea of this though. Many in group share like you too. Youngest was like baby but we really not want to go over 14/15 depends. But mainly for littles...is that okay?

Screenname 2: So you done a pic of her, live pic of panties. Then we laughing with the room. Once I get I send to main admins, they make final decisions and I add you when they say ok. I cant see it beings any problems 😊 Sometimes they tke a few to add. Im in UK so Im having time differentces with them.

Screenname 1: Gotcha. [Picture posted of a child's bedroom]

Screenname 1: Play room [Picture posted of a room]

Screenname 2: Great buddy. Ill send to admin for final and keep you posted. I tell them you a good guy for us, and a sexy girl. Lol.

Screenname 1: Thanks

Screenname 2: From what I can see little one has some sexy potential so I am sure they agree with me 😊



Screenname 1: [Picture posted which depicts the same girl as the earlier posted picture of the girl standing at the table. In this picture, the girl is wearing a pink nightgown with white hearts on it and is sitting on a small child's bed.]

Screenname 1: Let me know if I'm in

Screenname 2: I will 100%...cutey is welcome, and so is tiny PP guy 😊 I will message when I know

Screenname 1: [Picture posted which depicts a small female child sitting on the floor holding her toes while spreading her legs. The child's face is not visible but the child is wearing the same pink nightgown with white hearts on it as in the previous pictures. The child's vulva is clearly visible as the child is not wearing any underwear (attached under seal as Exhibit 1)]

11. As part of the investigation, I reviewed the records from Kik related to the "Screenname 1" account which showed the account was registered in November of 2020 and showed an unconfirmed email address associated with it. The records showed that the device used to register the account was an iPhone. The records also included a list of the IP addresses used to access the account from September 5, 2021, through September 10, 2021. I reviewed these records and noted that only one residential IP address, identified as 67.253.240.172 and assigned to Charter Communications, was used to



access the "Screenname 1" account during this period. As part of the investigation, HSI C3 received records from Charter Communications which provided subscriber information for IP address 67.253.240.172. These records showed that during the times it was used to access the "Screenname 1" account, the IP address was assigned to [REDACTED] [REDACTED] with the SUBJECT PREMISES listed as his address.

12. [REDACTED]

[REDACTED]

13. A search of the Accurant information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) was conducted for [REDACTED] [REDACTED]

[REDACTED]

14. [REDACTED]

[REDACTED]

15. On September 23, 2021, investigators conducted surveillance of the SUBJECT PREMISES and noted the tree directly in front of the residence has the number “364” affixed to it. While in the area of the SUBJECT PREMISES, investigators conducted a wireless survey and noted all of the wireless networks broadcasting were secure.

16. Based on the above, I have probable cause to believe, and I do believe, that [REDACTED] is the user of the “Screenname 1” Kik account and that he distributed child pornography on September 10, 2021, when he uploaded one child pornography image to the Kik chat group. As described below, the types of computing and storage devices capable of sending, receiving, and storing information relevant to the above-described crimes can be small, mobile, and easily hidden. They may therefore be found anywhere in the SUBJECT PREMISES, in any vehicles [REDACTED] has access to, or on his person.

17. As previously noted, Kik is an instant messaging application which sends and receives messages through mobile data or through an Internet connection and was designed to be used on mobile devices such as smart phones. I know that it is possible to install Kik on tablets and iPads as well. I also know through experience that it is possible to install Kik on other devices, such as laptop computers and desktop computers (all of the preceding devices will hereafter collectively be referred to as DEVICES) if the user installs additional free software which facilitates the Kik installation on that device. As such, I believe it probable any of these DEVICES could have accessed Kik and will

contain evidence of the "Screenname 1" Kik account installed and will also contain evidence of the Kik group "Screenname 1" participated in. I also believe it probable that these DEVICES will contain evidence of the image of child pornography "Screenname 1" uploaded to the Kik group. I believe a review of these DEVICES will establish who used them and who used the "Screenname 1" Kik account.

18. Based on the content of the Kik chat group in which "Screenname 1" participated, I have probable cause to believe, and I do believe, that "Screenname 1" has a sexual interest in children and that a review of the DEVICES will help establish that this sexual interest in children provided the motive for them to commit these crimes.

19. Based on my training and experience, I know that many of the DEVICES referenced above, which may contain contraband, fruits and evidence of crime, are by their very nature portable, this includes as example, but is not limited to, compact storage devices such as smart phones, laptop computers, and tablets. In my training and experience, I know it is not uncommon for individuals to keep these DEVICES on their person or in multiple locations within their premises, including in outbuildings and motor vehicles.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

20. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers and mobile devices, I know that data can be stored on a variety of systems and storage devices, including

external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage.

I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or

destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

21. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU).

22. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

**ELECTRONIC DEVICES, ELECTRONIC  
STORAGE, AND FORENSIC ANALYSIS**

23. As described above and in Attachment B, this application seeks permission to search for DEVICES and seize data and images that the DEVICES might contain,

which pertain to violations of 18 U.S.C. § 2252A. Some electronic data on the DEVICES may take the form of files, photographs, documents, and other data that is user-generated. Other data might become meaningful only upon forensic analysis. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or cell phone is evidence may depend on other information stored on the computer or cell phone and the application of knowledge about how the device behaves. Therefore, contextual information necessary to



understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. Based on my knowledge, training, and experience, I know that:

a. Files or remnants of files can be recovered months or even years after they have been downloaded onto an electronic device, deleted, or viewed via the Internet. Electronic files downloaded to an electronic device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes" a file from an electronic device, the data contained in the file does not necessarily disappear; rather, that data is no longer indexed but remains on the storage medium until it is overwritten by new data.

b. Wholly apart from user-generated files, electronic devices often contain electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and other files.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." These

files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

d. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how the DEVICES were used, the purpose of its use, who used it, where it was used, and when. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

e. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

f. The government intends to make and retain a full image copy of the seized media, so that a copy of the evidence, rather than the original evidence, can be examined. The government will seize and retain both the original evidence and any copies of this evidence. This procedure will ensure that the original evidence remains intact.

**REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT**

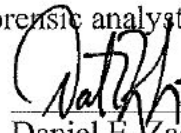
25. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

### **CONCLUSION**

26. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A,

authorizing the seizure and search of the items described in Attachment B.

27. I am aware that the recovery of data by a computer forensic analyst takes significant time. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.




Daniel E. Zaehring  
Special Agent  
Homeland Security Investigations

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedure

Date: Sep 23 2021

City and state: Bangor, ME



  
Judge's signature  
John C. Nilsson U.S. Magistrate Judge  
Printed name and title